



Professional Indemnity Insurance Risk Management Questionnaire

Your Firm

Practice Name:

Questions

1. Are employees able to work from home and still access relevant systems and files?
If 'Yes' please provide details.

Yes No

2. Is the business able to ensure that its usual risk management practices remain in place and are adhered to e.g. file audits, peer reviews, management of critical dates etc?
If 'Yes' please provide details.

Yes No

3. Is the business able to ensure that adequate 'know your customer' procedures and other fraud prevention measures are adhered to, especially where face-to-face meetings are not possible?
If 'Yes' please provide details.

Yes No

4. How does the business ensure that it maintains adequate cyber and data security when employees work away from company premises?

5. a) Who is responsible in the Practice for information security and provide her/his IT background?

- b) If you outsource the responsibility for information security, please provide the name and address of the third-party service provider

6. a) What firewall and malware protection systems do you have in place and how often are they reviewed and updated?

b) Do you always apply updates to critical IT systems and applications within 30 days of their release? Yes No

7. a) Do staff undergo information security and scam training? Yes No

**If 'Yes' please advise the type of training undertaken
e.g. social engineering including phishing, masquerading, other scams etc.**

b) How often does this take place?

c) Are all staff included? Yes No

8. If questions 7a) and/or 7c) are answered 'No' please explain why.

9. a) Do you restrict employees' and external users' privileges on a business need to know basis (particularly administrative permissions and access to sensitive data or personal data)? Yes No

b) Have you implemented a password policy enforcing the use of long and complex passwords across your organisation? Yes No

Long and complex passwords are defined as: *eight characters or more; free of consecutive identical, all-numeric or all-alphabetic characters.*

c) Is dual verification used to access the Company's system(s)? Yes No

If 'No' please describe your password policy, and confirm if you are able to introduce dual verification.

d) Do you revoke all system access, accounts and associated rights after termination of users (incl. partners, employees, temporary employees, contractors or vendors)? Yes No

10. What preparation has the business made in respect of unexpected staff absences, particularly in relation to senior staff?

11. How does the business manage any activities that normally require direct contact with clients?

12. How is the business managing its cashflow and what is its ability to continue trading with potential delays to and/or reductions in income?

13. What is the practice's business continuity plan to navigate any future pandemics and any similar scenarios?

14. In the event that the practice's caseload decreases, would it look to branch-out into any other areas of practice? Yes No
If yes, what types of work would be considered?

15. Are the business's supervisory controls able to be managed effectively despite changes to working practices?

Signed:

Date:

Print Name: